UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,581	12/05/2001	Roy F. Brabson	RSW920010223US1	3407

7590 04/19/2006

Jerry W. Herndon
IBM Corporation T81/503
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER	
PAN, JOSEPH T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/007,581	BRABSON ET AL.	
	Examiner	Art Unit	
	Joseph Pan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14,16-18,20 and 22-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14,16-18,20 and 22-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's Pre-Appeal Conference Request filed on January 23, 2006 has been carefully considered by a Pre-Appeal Conference. The conferees agreed that Arrow et al. do not explicitly teach that the offloading component is controlled by the operating system. Thus the finality of the Office Action mailed on October 20, 2005 is now withdrawn. The Office regrets any inconvenience caused by withdrawal of rejection. Claims 1-12, 14, 16-18, 20, 22-39 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 33-35 are rejected under 35 U.S.C. 103(a) as being anticipated by Arrow et al. (U.S. Patent No. 6,175,917) in view of Anand et al. (U.S. Patent No.: 6,370,599 B1).

Referring to claim 1:

i. Arrow et al. teach:

Receiving a first request at the operating system from the application programs to initiate a communication with a remote unit (see figure 1, element 140; column 6, lines 8-23, and column 7, lines 7-12 of Arrow et al.);

Providing a second request from the operating system to a security offload component which perform a security offload processing, the second request directing the security offload component to secure the communication with the remote

unit (see figure 1, elements 140, 145; column 6, lines 8-23, and column 7, lines 7-12 of Arrow et al.);

Providing a control function in the operating system for initiating operation of the security handshake processing by the security offload component (see figure 1, elements 140, 145; column 6, lines 8-23, and column 7, lines 7-12 of Arrow et al.).

However, Arrow et al. do not explicitly mention providing a control function in the operating system kernel to the security offload component.

ii. Anand et al. disclose a method for offloading specific processing tasks that would otherwise be performed in a computer system's processor and memory, to a peripheral device, or devices, that are connected to the computer (see abstract of Anand et al.), wherein the operating system ascertains the task offload capabilities of the peripheral hardware device, and enables the task offload capabilities of the peripheral hardware device (see figures 5-6; column 15, lines 48-56 ; and column 3, lines 24-60 of Anand et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Anand et al. into the system of Arrow et al. to provide a control function in the operating system kernel to the security offload component.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Anand et al. into the system of Arrow et al. to provide a control function in the operating system kernel to the security offload component, because "This offloading of computing tasks on a per-packet basis allows an application to selectively offload tasks on a dynamic, as-needed basis. As such, applications executing on the computer system processor are able to offload tasks in instances where it is busy processing other computing tasks and processor overhead is high. Multiple tasks can also be offloaded in batches to a particular peripheral." (see abstract, lines 26-28 of Anand et al.).

Referring to claim 2:

Arrow et al. and Anand et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). Arrow et al. further disclose executing the provided control function, thereby initiating operation of the security handshake processing (see column 9, lines 11-17 of Arrow et al.).

Referring to claim 3:

Arrow et al. and Anand et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). Arrow et al. further disclose that the operating system maintains control over operations of the security handshake process (see column 10, lines 53-56 of Arrow et al.).

Referring to claims 33-35:

i. Arrow et al. teach:

Providing a security offload component which performs security session establishment and control processing (see e.g. figure 1, element 145 of Arrow et al.);

Providing a control function in the operating system for initiating operation of the security session establishment and control processing by the security offload component (see e.g. figure 1, elements 140, 145; column 6, lines 8-23, and column 7, lines 7-12 of Arrow et al.).

Receiving a request at the operating system from the application program to initiate a communication with the remote unit (see figure 1, elements 140, 145; column 6, lines 8-23, and column 7, lines 7-12 of Arrow et al.).

Directing the security offload component to secure the communication with the remote unit in response to the request (see figure 1, elements 140, 145; column 6, lines 8-23, and column 7, lines 7-12 of Arrow et al.).

However, Arrow et al. do not explicitly mention providing a control function in the operating system kernel to the security offload component.

ii. Anand et al. disclose a method for offloading specific processing tasks that would otherwise be performed in a computer system's processor and

memory, to a peripheral device, or devices, that are connected to the computer (see abstract of Anand et al.), wherein the operating system ascertains the task offload capabilities of the peripheral hardware device, and enables the task offload capabilities of the peripheral hardware device (see figures 5-6; column 15, lines 48-56 ; and column 3, lines 24-60 of Anand et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Anand et al. into the system of Arrow et al. to provide a control function in the operating system kernel to the security offload component.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Anand et al. into the system of Arrow et al. to provide a control function in the operating system kernel to the security offload component, because "This offloading of computing tasks on a per-packet basis allows an application to selectively offload tasks on a dynamic, as-needed basis. As such, applications executing on the computer system processor are able to offload tasks in instances where it is busy processing other computing tasks and processor overhead is high. Multiple tasks can also be offloaded in batches to a particular peripheral." (see abstract, lines 26-28 of Anand et al.).

Referring to claims 36-37:

Arrow et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). Arrow et al. further disclose:

Preparing a data packet including data to be communicated to the remote unit (see column 7, lines 13-25 of Arrow et al.);

Reserving space in the data packet for security information (see column 7, lines 13-25 of Arrow et al.);

Passing the data packet including the reserved space to the security offload component (see column 7, lines 13-25 of Arrow et al.).

Referring to claim 38:

Arrow et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). Arrow et al. further disclose passing control information from the operating system to the security offload component, wherein the control information is passed to the security offload component separately from the data packet (see column 8, lines 4-11 of Arrow et al.).

Referring to claim 39:

Arrow et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). Arrow et al. further disclose:

Receiving the data packet at the security offload component (see column 7, lines 46-64 of Arrow et al.);

Encrypting the data in the data packet (see column 7, lines 46-64 of Arrow et al.);

Inserting security protocol information in the packet (see column 7, lines 46-64 of Arrow et al.);

Transmitting the resulting data packet to the remote unit (see column 7, lines 46-64 of Arrow et al.).

4. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917) in view of Anand et al. (U.S. Patent No.: 6,370,599 B1), and further in view of Brennan et al. (U.S. Patent No. 5,931,928).

Referring to claim 4:

i. Arrow et al. and Anand et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function (see claim 1 above). However, they do not specifically mention that the

operating system does not participate in operation of the security handshake processing.

ii. Brennan et al. disclose a system wherein the offload component will take over the handshake processing in lieu of the operating system (see column 27, lines 9-16 of Brennan et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Brennan et al. into the system of Arrow et al. and Anand et al. to let the offload security component to take over the security handshake processing.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Brennan et al. into the system of Arrow et al. and Anand et al. to let the offload security component to be active rather than passive role by taking over ongoing handshake processing from the operating system to ensure the successful handshake (see column 27, lines 16-27 of Brennan et al.). By offloading handshake task from the cpu, the system response time will be improved significantly.

5. Claims 5-6, 11-12, 14, 16-18, 20, 22-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917) in view of Anand et al. (U.S. Patent No.: 6,370,599 B1), further in view of Weinstein et al. (U.S. Patent No. 6,094,485).

Referring to claims 5-6:

i. Arrow et al. and Anand et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function (see claim 1 above). However, Arrow et al. and Anand et al. do not explicitly specify the information to be used by the security handshake processing.

ii. Weinstein et al. disclose a process for the client establishing a secure communication with the server via a SSL handshake, wherein Weinstein et al. disclose a connection such as TCP (see column 4, lines 51-53 of Weinstein et al.); a

protocol version to be used (see column 9, line 58 of Weinstein et al.); a security role of client or server (see column 3, lines 25-26 of Weinstein et al.); the cipher suites to be used for selection (see column 3, line 25-26 of Weinstein et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Weinstein et al. into the system of Arrow et al. and Anand et al. to specify the information needed for security handshake.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Weinstein et al. into the system of Arrow et al. and Anand et al. to specify the information needed for security handshake, since e.g. the SSL setup, which allows an exportable SSL client to negotiate an encrypted session using strong encryption with a server if the server is approved for the set up, i.e., if it is allowed to use strong encryption (see column 1, lines 35-39 of Weinstein et al.).

Referring to claim 11:

i. Arrow et al. and Anand et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control. However, Arrow et al. and Anand et al. do not specifically mention the operating system provides messages to be used in the handshake.

ii. Weinstein et al. disclose a process for the client establishing a secure communication with the server via a security handshake, wherein Weinstein et al. disclose that the operating system provides the messages to be used in the security handshake (see column 14, lines 20-24 of Weinstein et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Weinstein et al. into the system of Arrow et al. and Anand et al. to specify the messages needed for security handshake.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Weinstein et al. into the system of Arrow et al. and Anand et al. so that the operating system provides the messages used for security handshake, because the handshake protocol messages must be sent in certain format and order.

Sending handshake messages in an unexpected order results in a fatal error (see column 14, lines 53-55 of Weinstein et al.).

Referring to claim 12:

Arrow et al., Anand et al. and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose a client hello message in the handshake, and the client hello message includes a random number structure, which is used later in the process (see column 15, lines 17-18 of Weinstein et al.).

Referring to claim 14:

Arrow et al., Anand et al., and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose a server hello message in the handshake, and the server hello message includes a random number structure, which is used later in the process (see column 16, lines 35-41 of Weinstein et al.).

Referring to claims 16-17:

Arrow et al., Anand et al., and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose a client certificate (see column 18, line 60 of Weinstein et al.); and a server certificate (see column 17, line 1 of Weinstein et al.) to be used for the client-server security handshake.

Referring to claim 18:

Arrow et al., Anand et al., and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose client pre-master security secret (see column 19, lines 17-22 of Weinstein et al.).

Referring to claim 20:

Arrow et al., Anand et al., and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose that data encrypted with the public

key of a given key pair can only be decrypted with the private key (see column 8, lines 12-14 of Weinstein et al.).

Referring to claims 22-23:

Arrow et al., Anand et al., and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose the master secret (see column 9, line 9-10 of Weinstein et al.); the server write key and the client write key (see column 9, line 20-23 of Weinstein et al.).

Referring to claims 24-25:

Arrow et al., Anand et al., and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose using a digital signature to sign and validate messages transmitted between the client and the server (see column 18, lines 16-25 of Weinstein et al.).

Referring to claims 26-29:

Arrow et al., Anand et al., and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose using the message authentication code (MAC) to check the integrity of messages transmitted between the client and the server (see column 10, lines 39-42 of Weinstein et al.).

6. Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917) in view of Anand et al. (U.S. Patent No.: 6,370,599 B1), further in view of Brennan et al. (U.S. Patent No. 5,931,928), and further in view of Weinstein et al. (U.S. Patent No. 6,094,485).

Referring to claim 7:

i. Arrow et al. and Anand et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a

control function (see claim 1 above). However, Arrow et al. and Anand et al. do not specifically mention that the operating system does not participate in the security handshake processing. Arrow et al. and Anand et al. also do not explicitly specify the information used for the security handshake.

ii. Brennan et al. disclose a system wherein the offload component will take over the handshake processing in lieu of the operating system (see column 27, lines 9-16 of Brennan et al.). On the other hand, Weinstein et al. disclose a process for the client establishing a secure communication with the server via a security handshake, wherein Weinstein et al. disclose a connection such as TCP (see column 4, lines 51-53 of Weinstein et al.); a protocol version to be used (see column 9, line 58 of Weinstein et al.); a security role of client or server (see column 3, lines 25-26 of Weinstein et al.); the cipher suites to be used for selection (see column 3, line 25-26 of Weinstein et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Brennan et al. into the system of Arrow et al. and Anand et al. to let the offload security component take over the security handshake processing. And It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Weinstein et al. into the system of Arrow et al. and Anand et al. to specify the information needed for security handshake.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Brennan et al. into the system of Arrow et al. and Anand et al. to let the offload security component to be active rather than passive role by taking over ongoing handshake processing from the operating system to ensure the successful handshake (see column 27, lines 16-27 of Brennan et al.). By offloading the handshake task, which is often cpu-intensive, the overall system response time will be improved significantly. And the ordinary skilled person would have been motivated to have applied the teaching of Weinstein et al. into the system of Arrow et al. and Anand et al. to specify the information needed for security handshake, since e.g. the SSL setup, which allows an exportable SSL client to negotiate an encrypted session using strong

encryption with a server if the server is approved for the set up, i.e., if it is allowed to use strong encryption (see column 1, lines 35-39 of Weinstein et al.).

Referring to claim 8:

Arrow et al., Anand et al., Brenne et al. and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose the segment size (see column 9, lines 60-61 of Weinstein et al.), and the sequence numbers (see column 9, line 29 of Weinstein et al.) used in the security handshake processing.

7. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917) in view of Anand et al. (U.S. Patent No.: 6,370,599 B1), further in view of Brennan et al. (U.S. Patent No. 5,931,928), further in view of Weinstein et al. (U.S. Patent No. 6,094,485), and further in view of Gillon et al. (U.S. Patent No. 5,764,738).

Referring to claim 9:

i. Arrow et al., Anand et al., Brennan et al. and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function (see claim 7 above). However, they do not specifically mention that the offload component sends a message to the operating system upon completion of the handshake processing.

ii. Gillon et al. disclose a system wherein an offload component sends a message to a program upon completion of the handshake processing (see column 4, lines 37-42 of Gillon et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Gillon et al. into the system of Arrow et al., Anand et al., Brennan et al. and Weinstein et al. to send a message to the operating system upon completion of the handshake processing.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Gillon et al. into the system of Arrow et al., Anand et al., Brennan et al. and Weinstein et al. to send a message to the operating system upon completion of the handshake processing, so that the operating system can start using the secure communication set up by the security offload component.

Referring to claim 10:

Arrow et al., Anand et al., Brennan et al., Weinstein et al. and Gillon et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose the information available upon completion of the security handshake: the identifier of the secure session (see column 8, line 66 of Weinstein et al.); the server write key and the client write key (see column 9, line 20-23 of Weinstein et al.); the sequence numbers (see column 9, line 29 of Weinstein et al.); the cipher suite (see column 9, line 5-8 of Weinstein et al.); the protocol version (see column 9, lines 58-59 of Weinstein et al.); and the digital signature (see column 18, lines 16-25 of Weinstein et al.).

8. Claims 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917) in view of Anand et al. (U.S. Patent No.: 6,370,599 B1), further in view of Weinstein et al. (U.S. Patent No. 6,094,485), and further in view of Gillon et al. (U.S. Patent No. 5,764,738).

Referring to claim 30:

i. Arrow et al., Anand et al., and Weinstein et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function (see claim 11 above). However, they do not specifically mention that the offload component sends a message to the operating system upon completion of the handshake processing.

ii. Gillon et al. disclose a system wherein an offload component sends a message to a program upon completion of the handshake processing (see column 4, lines 37-42 of Gillon et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Gillon et al. into the system of Arrow et al. Anand et al., and Weinstein et al. to send a message to the operating system upon completion of the handshake processing.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Gillon et al. into the system of Arrow et al., Anand et al., and Weinstein et al. to send a message to the operating system upon completion of the handshake processing, so that the operating system can start using the secure communication set up by the security offload component.

Referring to claim 31-32:

Arrow et al., Anand et al., Weinstein et al. and Gillon et al. teach the claimed subject matter: providing a security offload component which performs security handshake, and a control function. Weinstein et al. further disclose the information available upon completion of the security handshake: the identifier of the secure session (see column 8, line 66 of Weinstein et al.); the server write key and the client write key (see column 9, line 20-23 of Weinstein et al.); the sequence numbers (see column 9, line 29 of Weinstein et al.); the cipher suite (see column 9, line 5-9 of Weinstein et al.); the protocol version (see column 9, lines 58-59 of Weinstein et al.); and the digital signature (see column 18, lines 16-25 of Weinstein et al.).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-6300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan
April 17, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100